ManageEngine
ADManager Plus

5 IGA essentials

to ensure security and compliance in your organization

www.admanagerplus.com

Table of Contents

1

Preface

The IT industry is growing at a rate of 6-7% every year. This growth can be attributed to a variety of factors, including a rise in the availability and use of SaaS applications and other cloud offerings, developments in IoT and AI, as well as widespread adoption of hybrid and remote-first workplace models. However, this growth carries a cost. Breaking the distance and business barriers has made organizations vulnerable to cyberattacks. While organizations are still catching up with their network perimeter expansion, cybercriminals are exploiting the loopholes and developing sophisticated tools and techniques to gain access to organizational resources. Adding to the financial loss of a data breach, these attacks can damage a brand's image and lead to a loss of customer loyalty. For these reasons, organizations should focus on securing their network not only from outsiders, but from the individuals who already have access.

2

Identity-based cyberattacks

Despite organizations following the best security practices and deploying defensive systems to secure their network, many still fall victim to cyberattacks. This is because organizations still largely depend on "corporate identities" for authentication and authorization, and these identities can be easily compromised. Attacks on corporate identities have increased as workplaces have adapted to hybrid and remote setups, expanding corporate perimeters beyond an organization's premises.

When users were limited to using office machines, password-based authentication was considered as a good enough security measure. Now users are logging in from practically anywhere—sometimes using their own devices under a BYOD policy—blurring corporate perimeters and making them only as strong as the identities and verification methods used.

The credentials that we use to access the devices and accounts are being exploited by cyber criminals. Let's look into two of the most common yet impactful identity-based cyberattacks: credential stuffing and password spraying.

Credential stuffing is one of the more complicated identity-based cyberattacks. This is where an attacker gets a large list of user credentials from any password dump site, breached website, or even from the dark web. Hackers will test these stolen credentials in an effort to victimize corporate networks. Credential stuffing is largely successful because of users' poor password hygiene. According to a survey, the average American has 130 accounts linked to an email and it is not practical to create a new password for each of them. The experience of password fatigue, as well as the inclination to use common passwords, can easily lead to major security risks.

Password spraying is another identity-based brute force attack that's becoming increasingly prevalent. In this technique, an attacker uses a single password against multiple user accounts in a network. The attacker is trying to simultaneously log into multiple accounts using the same password to increase their chances of breaking in. This method doesn't usually trigger account lockouts in the same way other brute force attacks do, making it harder to detect. The hackers succeed with this method because users tend to not be innovative with their passwords. For example, according to pwned passwords, password1 has appeared in data breaches 3.2 million times.

Identity-based attacks can be largely avoided if enterprises focus on keeping good password hygiene and optimize their identity management. The next section focuses on why security should be driven based on identity and how to achieve holistic network security using identity management techniques.

3 Identity management and identity-based security

Identity management ensures that only authorized users can access their organization's resources, and only the resources that they absolutely require to perform their job functions. With identity management in place, users are granted access to privileged resources by authenticating them not only with their credentials, but with an additional factor such as a one-time passcode or biometric scan. This ensures security and prevents unauthorized access in case of an account compromise.

Identity-based security provides a structure to how identities can be audited to ensure every base is covered. Adopting this approach will make organizations future-ready, where identity will become the core of security. As an additional layer of precaution, the right time and right access methods can be added and organizations can implement Zero Trust principles to secure their network.

Guaranteeing users have least-privilege access to resources (i.e. providing access only when it is required) can prevent unauthorized access at the root itself.

4 IGA: What, why, and how

To establish an identity-based security strategy, one of the important frameworks required is identity governance and administration (IGA), which is a part of identity and access management (IAM). IGA enables organizations to secure and govern identities by more or less combining identity governance (which provides improved visibility into user access, segregation of duties, role-based access, workflow management, analytics, and reporting) with identity administration (which includes provisioning and de-provisioning, user account management, credentials management, and user and privilege management).

As an organization grows in size, it is easy for admins to lose track of the happenings with respect to each identity. When implemented properly, IGA enables IT admins to seamlessly manage user identities and their access rights. It improves visibility into every single user, including their access rights, thereby allowing IT admins to implement the necessary controls to prevent any unauthorized access.

IGA has become all the more essential after hybrid workforces have became the new norm. Organizations are going digital and moving away from an on-premises approach and toward a multi-cloud or hybrid IT approach to avoid concentration risks. This places additional load on the IT team to manage the security posture of the organization while juggling between various cloud environments.

IT ecosystems have grown in complexity, with the expansion of the corporate network and increases in the number of platforms used. These changes have made corporate networks more vulnerable to breaches. Having IGA in place will help IT admins to provide the right level of access to each individual, thereby ensuring good user experience and security of the network.

5

Five IGA essentials and why ManageEngine ADManager Plus is the perfect fit for your IGA requirements

Out of all the critical capabilities recommended by Gartner for IGA, there are 5 essential capabilities:

1. Identity lifecycle management
2. Role-based access
3. Privileged access management
4. Workflow automation
5. Reporting

These 5 capabilities are easily handled by ManageEngine ADManager Plus, which is a unified management and reporting solution for Active Directory (AD), Microsoft 365, Exchange, Skype for Business, and Google Workspace. It allows IT admins to manage AD objects and generates an exhaustive list of AD reports, all from a single console.

1. Identity lifecycle management

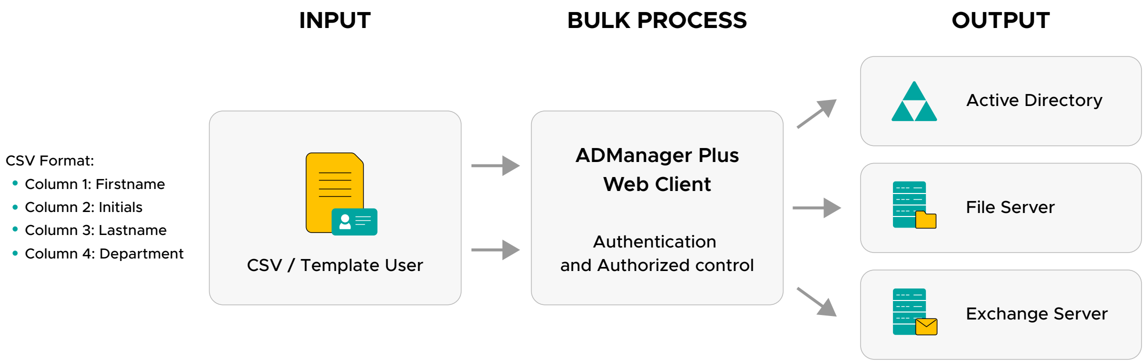
Identity lifecycle management is the process of managing user accounts throughout their entire lifecycle (i.e. starting with account creation when joining the organization and ending with de-provisioning when leaving). For example, assume an account is created for an employee with certain permissions which tend to change as the employee's journey in the company changes. Some permissions given at the time of joining may have to be revoked and new access may be required. Lastly, at the time of their leaving, the account should be deactivated first, then archived, and later deleted.

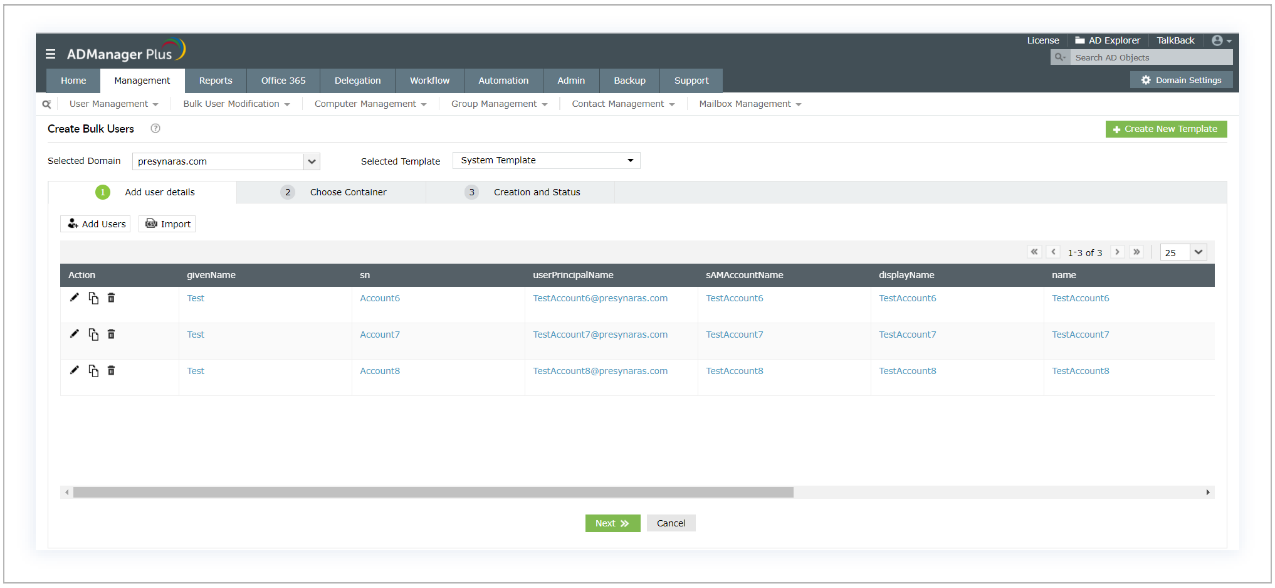
All these may sound simple and it's maybe possible to manually address each step in smaller organizations. But in mid-sized and large organizations these tasks will take a lot of time and an IT admin would have to manage accounts amidst their other essential tasks. What's more, skipping any of these steps could have disastrous outcomes. For example, deleting the account is a crucial step due to many data breaches happening through an inactive account.

ADManager Plus lifecycle management

With ADManager Plus' lifecycle management feature, everything from provisioning to de-provisioning can be done from a single console. It enables the system administrators to manage the daily tasks of creating new employee identities, removing old permissions, managing the changes in existing identities, and so on. It also allows provisioning users simultaneously to other tools such as Microsoft 365, Exchange, Skype for Business, and Google Workspace. The fact that IT admins can delegate tasks to non-technicians via the tool in a completely secure manner eases the burden of IT admins from performing mundane tasks.

The tool also allows users to create and modify users in bulk and configure their general attributes and automate the routine tasks with defined automation policies on multiple platforms—such as AD, Microsoft 365, Exchange, Skype for Business, and Google Workspace—with customized settings for each platform.





Create Bulk Users

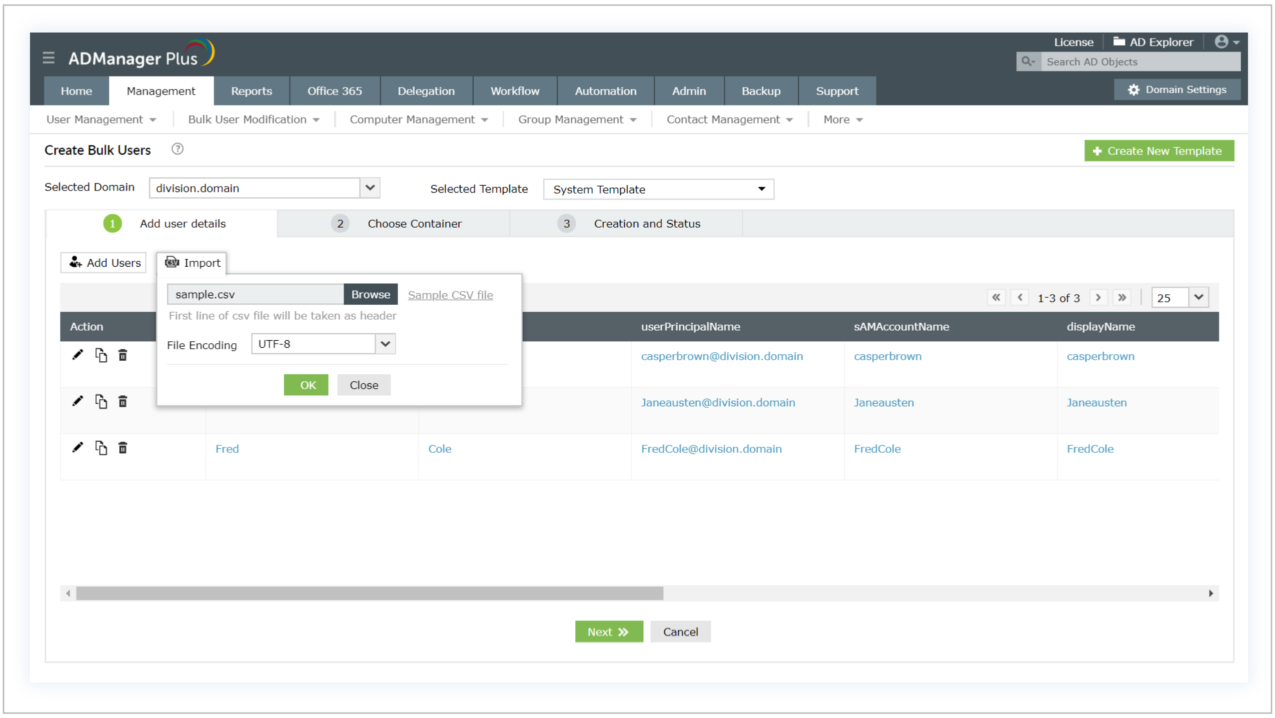
Selected Domain: presynaras.com

Selected Template: System Template

1 Add user details | 2 Choose Container | 3 Creation and Status

1-3 of 3 | 25

Action	givenName	sn	userPrincipalName	sAMAccountName	displayName	name
	Test	Account6	TestAccount6@presynaras.com	TestAccount6	TestAccount6	TestAccount6
	Test	Account7	TestAccount7@presynaras.com	TestAccount7	TestAccount7	TestAccount7
	Test	Account8	TestAccount8@presynaras.com	TestAccount8	TestAccount8	TestAccount8



Create Bulk Users

Selected Domain: division.domain

Selected Template: System Template

1 Add user details | 2 Choose Container | 3 Creation and Status

sample.csv

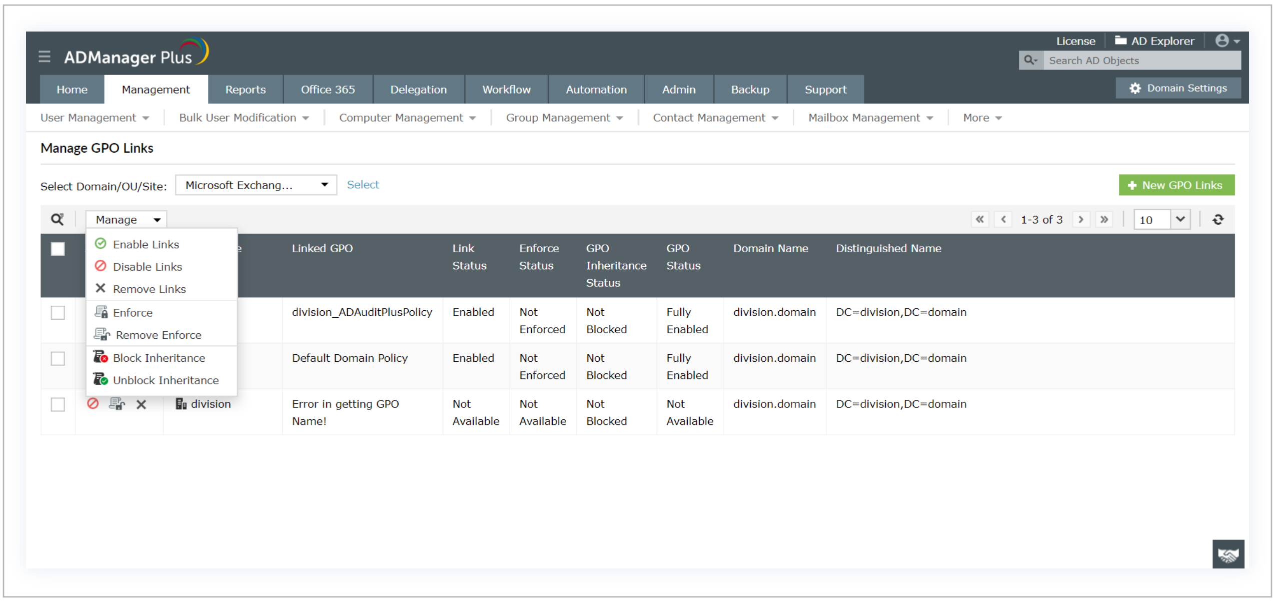
First line of csv file will be taken as header

File Encoding: UTF-8

1-3 of 3 | 25

Action			userPrincipalName	sAMAccountName	displayName
			casperbrown@division.domain	casperbrown	casperbrown
			Janeausten@division.domain	Janeausten	Janeausten
	Fred	Cole	FredCole@division.domain	FredCole	FredCole

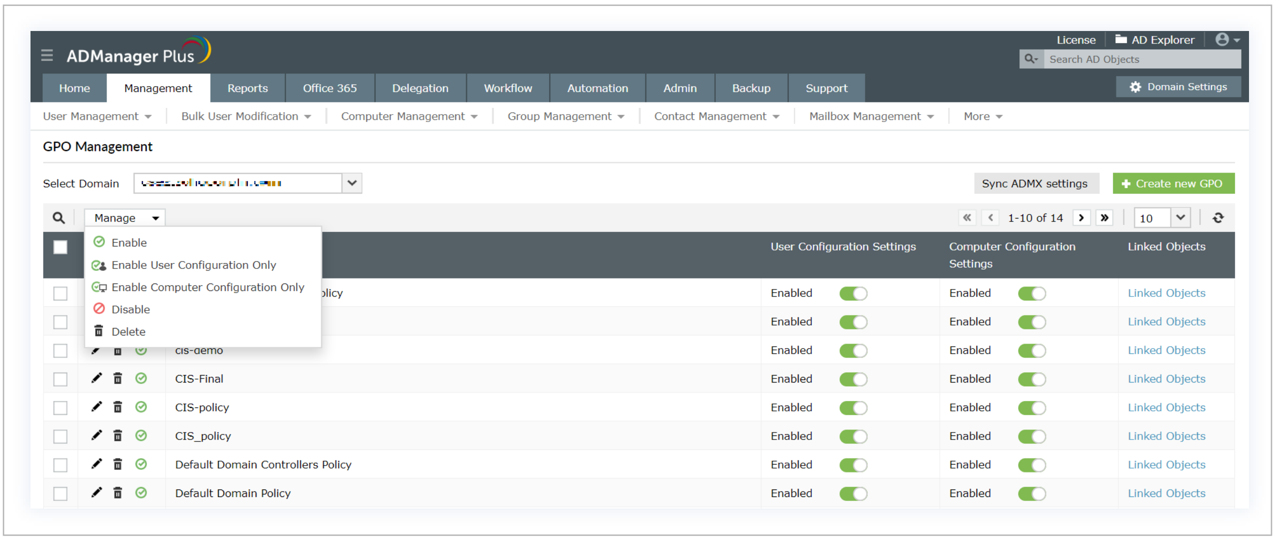
ADManager Plus helps manage AD users, computers, and groups easily without having to rely on AD Group Policy management tools or PowerShell, both of which can be mundane and time-consuming. It allows Group Policy Objects (GPOs) of multiple domains to be managed in just a few clicks. With ADManager Plus, GPOs can be created and linked to any container at once, as well as deleted, enabled, or disabled in bulk.



Manage GPO Links

Select Domain/OU/Site: Microsoft Exchang... Select

			Linked GPO	Link Status	Enforce Status	GPO Inheritance Status	GPO Status	Domain Name	Distinguished Name
□			division_ADAuditPlusPolicy	Enabled	Not Enforced	Not Blocked	Fully Enabled	division.domain	DC=division,DC=domain
□			Default Domain Policy	Enabled	Not Enforced	Not Blocked	Fully Enabled	division.domain	DC=division,DC=domain
□	⊘ ✕	division	Error in getting GPO Name!	Not Available	Not Available	Not Blocked	Not Available	division.domain	DC=division,DC=domain



GPO Management

Select Domain [redacted]

			User Configuration Settings	Computer Configuration Settings	Linked Objects
□		olicy	Enabled	Enabled	Linked Objects
□			Enabled	Enabled	Linked Objects
□		cis-demo	Enabled	Enabled	Linked Objects
□	✓	CIS-Final	Enabled	Enabled	Linked Objects
□	✓	CIS-policy	Enabled	Enabled	Linked Objects
□	✓	CIS_policy	Enabled	Enabled	Linked Objects
□	✓	Default Domain Controllers Policy	Enabled	Enabled	Linked Objects
□	✓	Default Domain Policy	Enabled	Enabled	Linked Objects

2. Role-based access

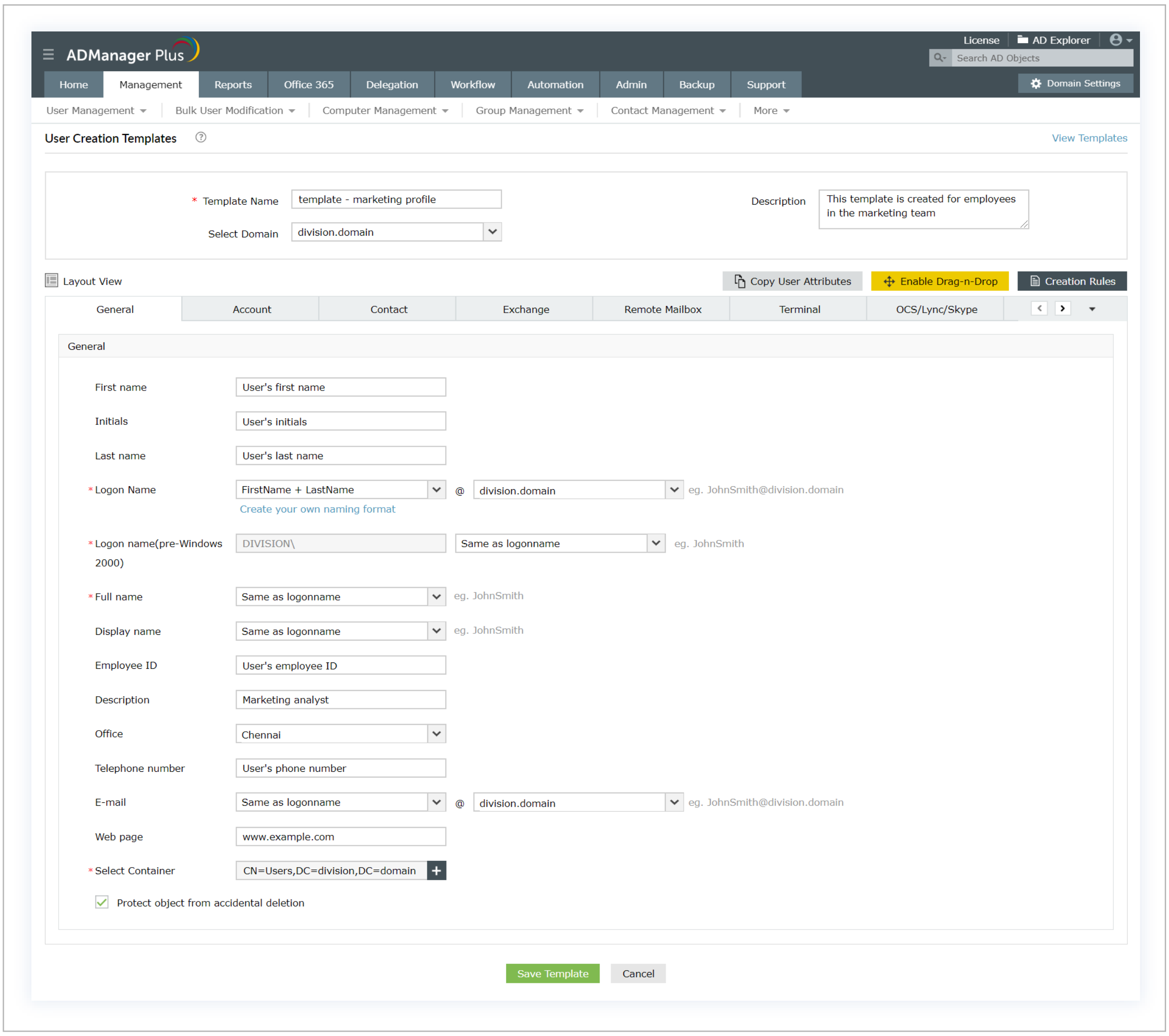
Role-based access is the method of restricting user access based on their job roles. The advantages of role-based access are:

1. Smoother operation for employees as they will get all the access rights they need by default, ensuring productivity from day one.
2. Ensures that every user can access only the resources they absolutely need and cannot access the ones that don't pertain to them. This results in increased security by ensuring employees down the ladder do not have access to privileged data.

Hence, deploying this IGA capability will provide a multitude of benefits to an organization. Besides being able to secure critical applications and sensitive data better, it will improve the operational efficiency every time an employee joins by providing them with necessary access by default.

ADManager Plus role-based access

ADManager Plus' role-based access capabilities will help IT admins create, modify, and delete users' roles based on organizational requirements. All the necessary attributes for a particular role can be defined and applied to every person assigned that role. The templates for individual roles have pre-defined settings for the user member's access rights, emails, group memberships, etc.



User Creation Templates

* Template Name: template - marketing profile

Select Domain: division.domain

Description: This template is created for employees in the marketing team

General

First name: User's first name

Initials: User's initials

Last name: User's last name

*Logon Name: FirstName + LastName @ division.domain eg. JohnSmith@division.domain

*Logon name(pre-Windows 2000): DIVISION\ Same as logonname eg. JohnSmith

*Full name: Same as logonname eg. JohnSmith

Display name: Same as logonname eg. JohnSmith

Employee ID: User's employee ID

Description: Marketing analyst

Office: Chennai

Telephone number: User's phone number

E-mail: Same as logonname @ division.domain eg. JohnSmith@division.domain

Web page: www.example.com

*Select Container: CN=Users,DC=division,DC=domain

☑ Protect object from accidental deletion

3. Privileged access management

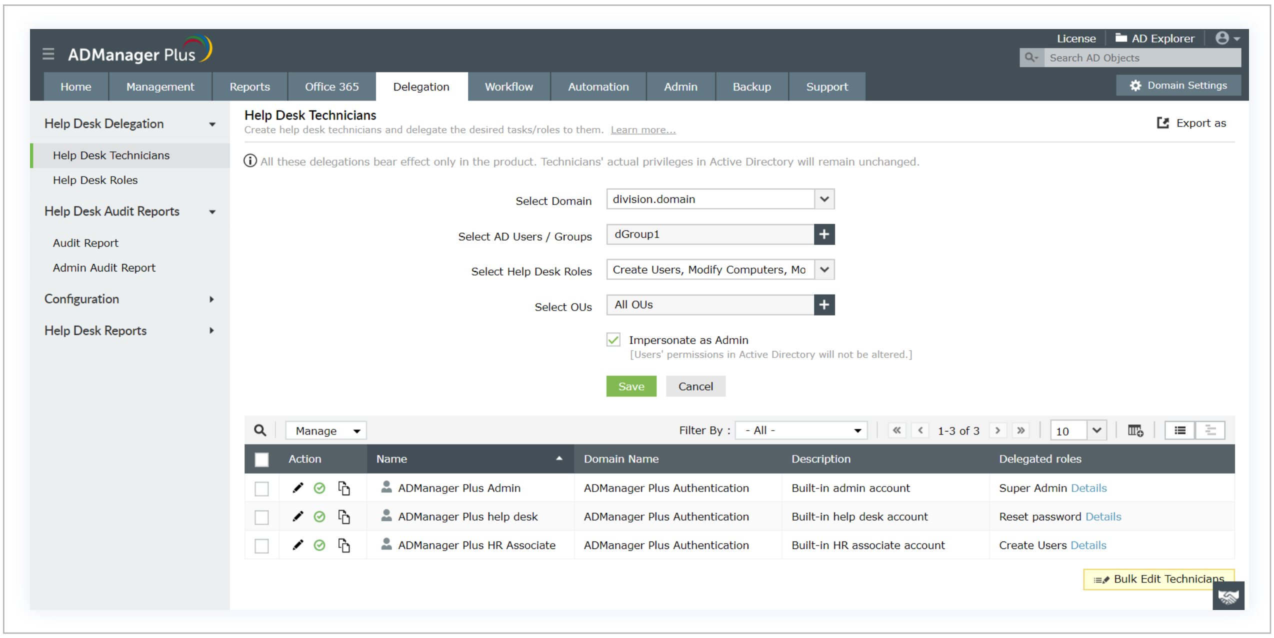
Privileged access management (PAM) is the process of making sure that unauthorized people do not have access to the most important resources of an organization. Defining who has access to particular resources is the first line of defense against potential threats, particularly attacks made to privileged users, such as C-level executives, managing directors, and VPs. These privileged users will have access to sensitive data of the organization and hold rights to perform certain administrative and definitive functions, similar to IT admins being able to block, restrict, or delete users' accounts or revoke access, while technicians cannot perform those actions.

Since sensitive information of an organization is reserved for access by certain people, PAM helps to create a secure environment for such information. PAM does that by isolating sensitive information from the rest of the members and provides access to only the privileged members. Periodic access review is also a crucial part of PAM. The access rights of privileged users are provided selectively, monitored, and periodically reviewed to ensure security is always maintained. More than just securing data, PAM ensures that users only have the least privileged access, meaning they only get to access what they absolutely need to perform their job functions.

ADManager Plus privileged access management

ADManager Plus provides various reports and access control functionalities for all the above discussed PAM capabilities. It helps to identify the number of users with access to privileged accounts and detailed reports on what they can access. Users' rights can be temporarily elevated and set to be revoked automatically after a specified period. The tool also helps identify improper, accidental, and even malicious changes made by privileged users and administrators by auditing their activities.

ADManager Plus also helps to manage the privilege access for group memberships. It helps track the scope of groups and the inherent permissions a user has in such groups. The tool helps by providing visibility into groups without members, groups with members, members of a group including nested groups, and more.



Help Desk Technicians
Create help desk technicians and delegate the desired tasks/roles to them. Learn more...

ⓘ All these delegations bear effect only in the product. Technicians' actual privileges in Active Directory will remain unchanged.

Select Domain: division.domain

Select AD Users / Groups: dGroup1

Select Help Desk Roles: Create Users, Modify Computers, Mo

Select OUs: All OUs

☑ Impersonate as Admin
[Users' permissions in Active Directory will not be altered.]

Filter By : - All - 1-3 of 3 10

□	Action	Name	Domain Name	Description	Delegated roles
□		ADManager Plus Admin	ADManager Plus Authentication	Built-in admin account	Super Admin Details
□		ADManager Plus help desk	ADManager Plus Authentication	Built-in help desk account	Reset password Details
□		ADManager Plus HR Associate	ADManager Plus Authentication	Built-in HR associate account	Create Users Details

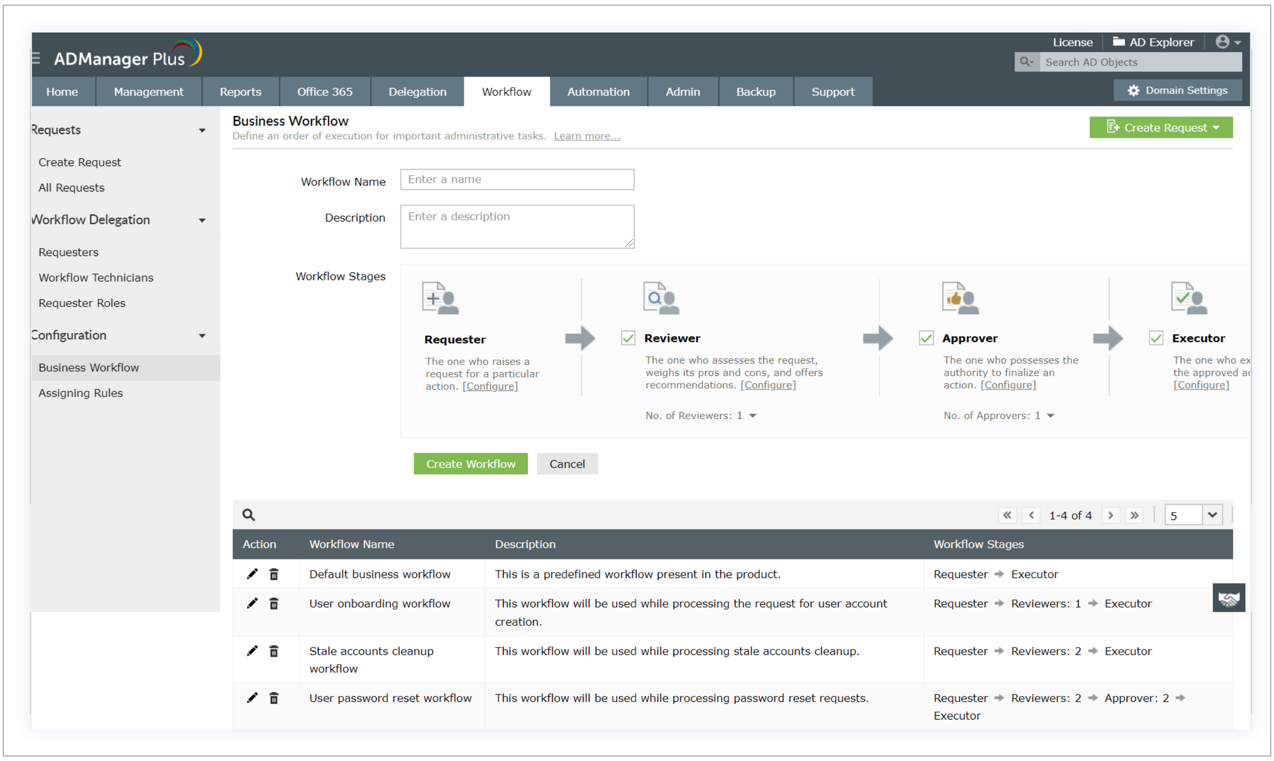
4. Workflow automation

Workflow is the deployment of a pre-decided flow of functions from lower-access users to the higher access ones. This enables easier flow of approval and reduces everyday friction. The IT administrator defines the workflow for all the activities like account creation, account modification, password resets, and so on. Once established and approved, all processes falling under a particular category go through the pre-defined workflow for that category.

When designed and implemented the right way, workflows can result in operational efficiencies, reduced manual efforts, easier audits, and also decrease the associated costs in the long run. Automated workflows make it easy for even new users to request access to the systems.

ADManager Plus workflow automation

With ADManager Plus, standard workflows can be created for all the tasks in an organization and can be customized based on need. Each workflow can involve four levels of workflow agents: requesters, reviewers, approvers, and executors. With clearly defined work roles, tasks can have clearly defined workflow without any conflict of roles.



Business Workflow

Define an order of execution for important administrative tasks. Learn more...

Workflow Name: Enter a name

Description: Enter a description

Workflow Stages

Requester The one who raises a request for a particular action. [Configure]

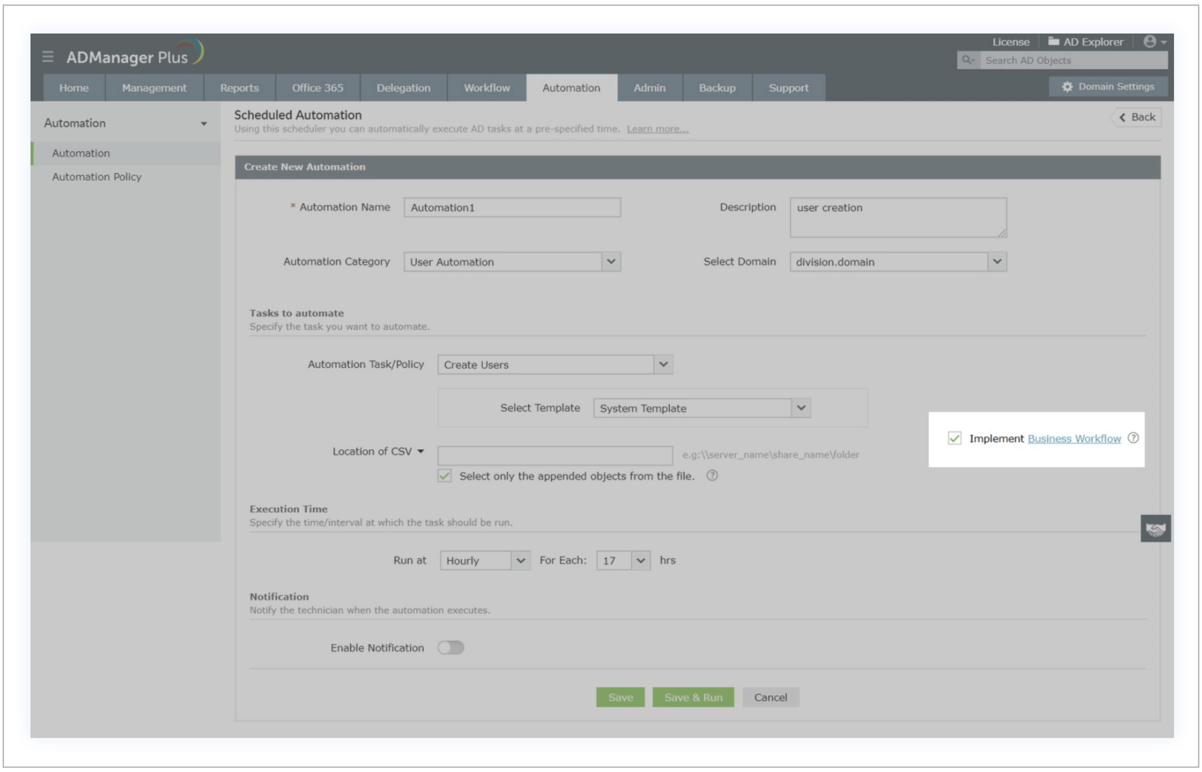
☑ **Reviewer** The one who assesses the request, weighs its pros and cons, and offers recommendations. [Configure]
No. of Reviewers: 1

☑ **Approver** The one who possesses the authority to finalize an action. [Configure]
No. of Approvers: 1

☑ **Executor** The one who ex the approved a [Configure]

Action	Workflow Name	Description	Workflow Stages
	Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
	User onboarding workflow	This workflow will be used while processing the request for user account creation.	Requester → Reviewers: 1 → Executor
	Stale accounts cleanup workflow	This workflow will be used while processing stale accounts cleanup.	Requester → Reviewers: 2 → Executor
	User password reset workflow	This workflow will be used while processing password reset requests.	Requester → Reviewers: 2 → Approver: 2 → Executor

ADManager Plus allows for automating repetitive and time consuming Active Directory tasks to save time and improve efficiency. The tool identifies 14 crucial and repeated AD tasks across four categories—User Creation, User modification, Group Modification, and Computer and Contact Management—and offers controlled automation for each. It allows specific templates to be created for each process with prebuilt actions, which can be run every time to save time and avoid manual error.



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1

Description: user creation

Automation Category: User Automation

Select Domain: division.domain

Tasks to automate
Specify the task you want to automate.

Automation Task/Policy: Create Users

Select Template: System Template

☑ Implement Business Workflow

Location of CSV: e.g:\\server_name\share_name\folder

☑ Select only the appended objects from the file.

Execution Time
Specify the time/interval at which the task should be run.

Run at: Hourly For Each: 17 hrs

Notification
Notify the technician when the automation executes.

Enable Notification

ADManager Plus also gives a complete summary of any pre-defined task: this includes all the relevant information like the time at which execution of the task began, who is the requester of the task, who are the workflow agents assigned, the current workflow status, and so on. An electronic document of all tasks executed and accesses that occurred helps in being compliant and staying vigilant over the long run.

ADManager Plus also enhances communication between users. Conditional rules can be set to allocate resources or technicians based on a task's priority. Workflow agents can also be set to be intimated regarding the requests that have been raised, reviewed, or approved.

5. Reporting

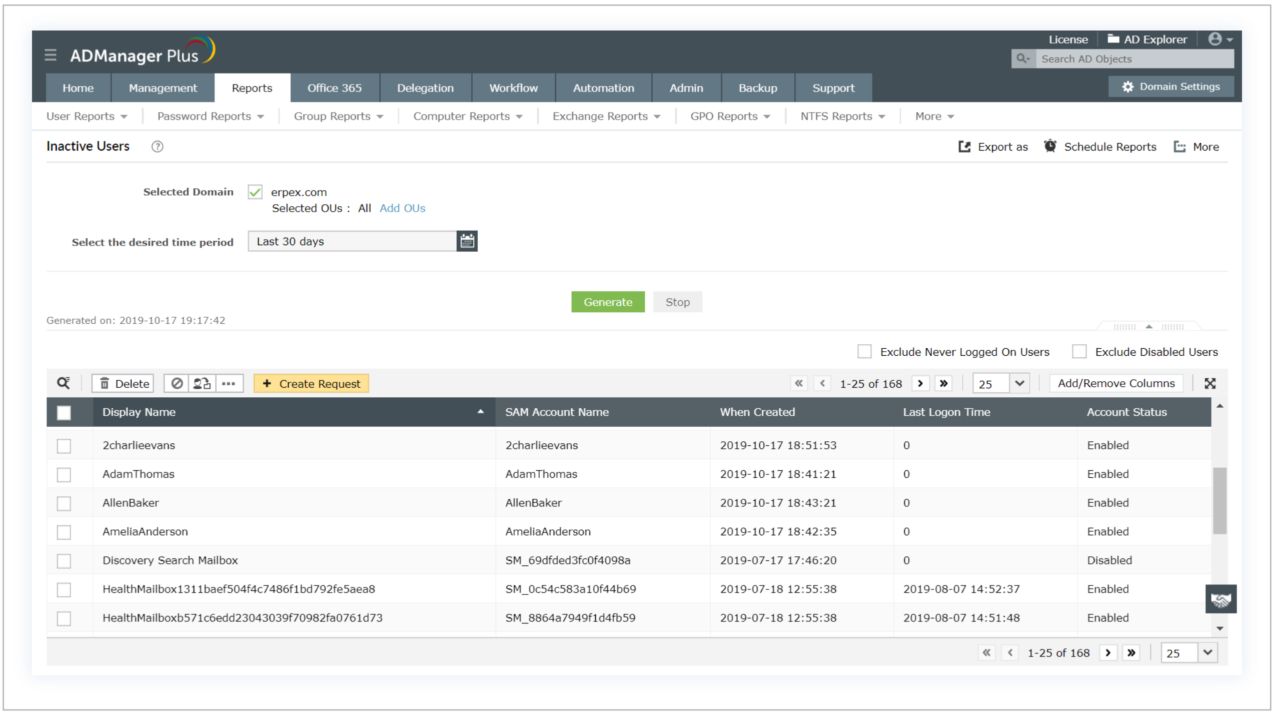
Reporting comes in handy when an organization grows in size, which often results in increasing amounts of data being generated alongside an increasing user base. In such cases, identifying, analyzing, and monitoring such large data can be handled using reporting and analytics.

Reporting software with an interactive dashboard provides a bird's eye view of all the major occurrences that need to be periodically reviewed. IT admins can select, view, analyze, summarize, and act upon just the data that they need. User reports give complete visibility to Windows Active Directory domains to monitor and manage the user accounts proactively and efficiently, which becomes tedious otherwise. Additional features like customizable reports and creative visualizations can help them take quick actions with the loads of data that they receive on a daily basis.

ADManager Plus reporting

ADManager Plus has a highly functional, customizable report generating capability that is fully web based. The reporting tool has more than 200 report templates which can be used to summarize and generate all types of reports on information regarding users, groups, group memberships, user logon, passwords, access rights, e-mail addresses, file permissions, and so on. It can export the reports in various formats like CSV, XLS, etc., and the report generation can be scheduled and automated as well. It has a user-friendly interface that enables even non-IT users to generate and view reports with ease.

ADManager Plus can also generate reports on Exchange Online and Exchange Server mailboxes, Microsoft 365, Google Workspace, Skype for Business (formerly Lync and LCS), and more—all from the single console. Compliance reports can also be generated for SOX,HIPAA, and more.



Inactive Users

Selected Domain ☑ erpex.com
Selected OUs : All Add OUs

Select the desired time period: Last 30 days

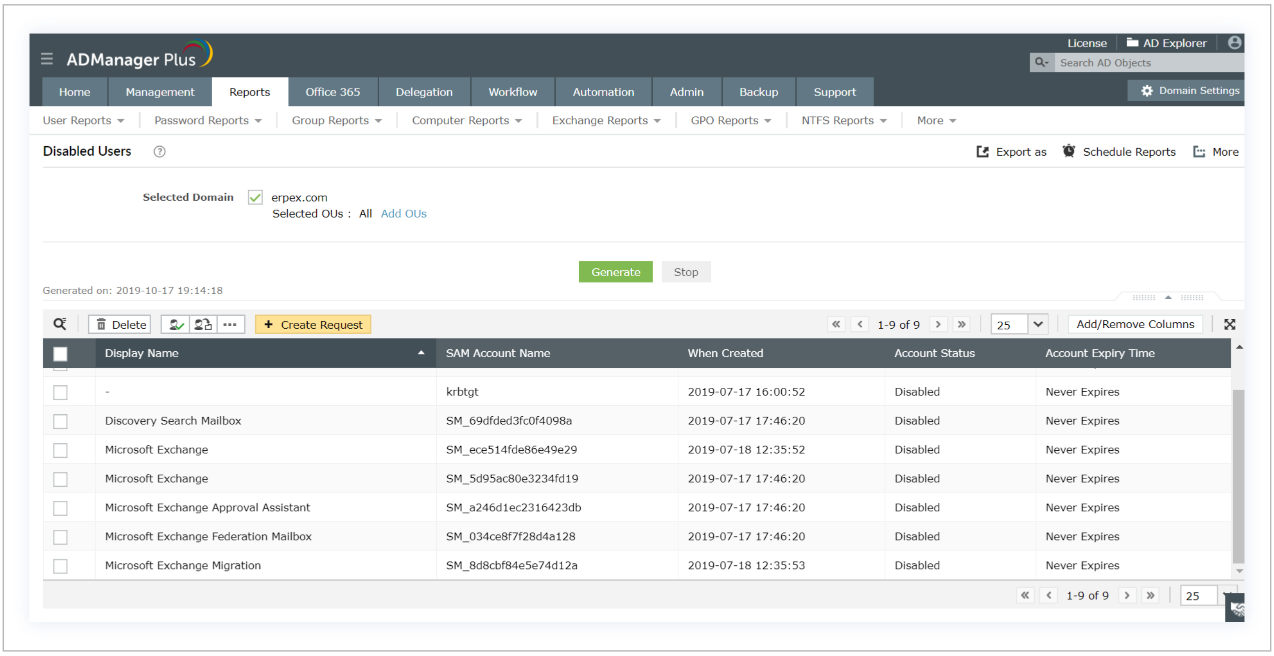
Generated on: 2019-10-17 19:17:42

□ Exclude Never Logged On Users □ Exclude Disabled Users

1-25 of 168 | 25

□	Display Name	SAM Account Name	When Created	Last Logon Time	Account Status
□	2charlieevans	2charlieevans	2019-10-17 18:51:53	0	Enabled
□	AdamThomas	AdamThomas	2019-10-17 18:41:21	0	Enabled
□	AllenBaker	AllenBaker	2019-10-17 18:43:21	0	Enabled
□	AmeliaAnderson	AmeliaAnderson	2019-10-17 18:42:35	0	Enabled
□	Discovery Search Mailbox	SM_69dfded3fc0f4098a	2019-07-17 17:46:20	0	Disabled
□	HealthMailbox1311baef504f4c7486f1bd792fe5aea8	SM_0c54c583a10f44b69	2019-07-18 12:55:38	2019-08-07 14:52:37	Enabled
□	HealthMailboxb571c6edd23043039f70982fa0761d73	SM_8864a7949f1d4fb59	2019-07-18 12:55:38	2019-08-07 14:51:48	Enabled

1-25 of 168 | 25



Disabled Users

Selected Domain ☑ erpex.com
Selected OUs : All Add OUs

Generated on: 2019-10-17 19:14:18

1-9 of 9 | 25

□	Display Name	SAM Account Name	When Created	Account Status	Account Expiry Time
□	-	krbtgt	2019-07-17 16:00:52	Disabled	Never Expires
□	Discovery Search Mailbox	SM_69dfded3fc0f4098a	2019-07-17 17:46:20	Disabled	Never Expires
□	Microsoft Exchange	SM_ece514fde86e49e29	2019-07-18 12:35:52	Disabled	Never Expires
□	Microsoft Exchange	SM_5d95ac80e3234fd19	2019-07-17 17:46:20	Disabled	Never Expires
□	Microsoft Exchange Approval Assistant	SM_a246d1ec2316423db	2019-07-17 17:46:20	Disabled	Never Expires
□	Microsoft Exchange Federation Mailbox	SM_034ce8f7f28d4a128	2019-07-17 17:46:20	Disabled	Never Expires
□	Microsoft Exchange Migration	SM_8d8cbf84e5e74d12a	2019-07-18 12:35:53	Disabled	Never Expires

1-9 of 9 | 25

The move towards hybrid and remote-first workplaces has expedited the rapid adoption of SaaS and cloud technology. This has given an added responsibility to IT admins of securing their user identities, no matter where those users work from. Deploying the 5 IGA essentials discussed in this book is a good place to start for organizations, as these are also recommended by Gartner.

As explored above, ManageEngine ADManager Plus can help with implementing and maintaining IGA. Book a demo to find out how.

Get in touch for demo

About ManageEngine ADManager Plus

ManageEngine ADManager Plus is a web-based Windows Active Directory management and reporting solution that helps Active Directory administrators and help desk technicians accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks, like AD object backup and recovery, and generates an exhaustive list of Active Directory reports, many of which are essential requirements for satisfying compliance audits. It also helps administrators manage and report on their Exchange Server, Office 365, G Suite, and Active Directory environments—all from a single console.

$ Get Quote

⤓ Download